	AUSA: Andrew Yahkind	Telephone: (313) 226-9565
AO 91 (Rev. 11/11) Criminal Complaint	Special Agent: ☑ Elizabeth Weitzel	Telephone: (313) 505-7304

UNITED STATES DISTRICT COURT
for the

Eastern District of Michigan

United States of America
v.
Ray Anthony Eddington

Case No.

Case: 2:23–mj–30026
Assigned To : Unassigned
Assign. Date : 1/25/2023
SEALED MATTER (LH)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of _____ April 2020 _____ in the county of _____ Wayne _____ in the _____ Eastern _____ District of _____ Michigan _____, the defendant(s) violated:

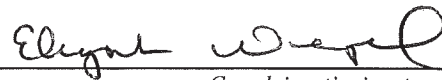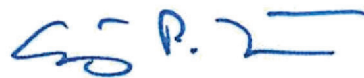| Code Section	Offense Description
18 U.S.C. § 1343	wire fraud
18 U.S.C.§ 1349	conspiracy to commit wire fraud
18 U.S.C. § 1028A	aggravated identity theft

This criminal complaint is based on these facts:

☐ Continued on the attached sheet.

Complainant's signature

Elizabeth Weitzel, Special Agent
Printed name and title

Sworn to before me and signed in my presence
and/or by reliable electronic means.

Date: _____ January 25, 2023 _____

City and state: _Detroit, MI_

Judge's signature

Hon. Anthony P. Patti   United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF A COMPLAINT

I, Elizabeth Weitzel, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1.   I am a Special Agent of the U.S. Department of Labor, Office of Inspector General, Office of Investigations - Labor Racketeering and Fraud (DOL-OIG/OI-LRF) and have been so employed since May of 2021. Prior to this assignment, I was a Special Agent with the U.S. Department of Housing and Urban Development Office of Inspector General (HUD OIG), for over 11 years. I am currently assigned to the Detroit Field Office of DOL OIG and to the Federal Bureau of Investigation (FBI) Detroit Metropolitan Identity Theft and Financial Crimes Task Force (DMIFT). I have conducted numerous criminal fraud investigations involving identity theft, financial, and unemployment fraud schemes. I was previously assigned to the Southeast Michigan Financial Crimes Task Force. I have conducted and/ or assisted numerous search and arrest warrants related to these violations. I have additional experience and training from the Federal Law Enforcement Training Center regarding criminal activity, economic crimes, and identity theft.

2.   Prior to my employment with HUD OIG, I was a Corporate Investigator and Bank Officer from July of 2006 until March of 2010. I investigated cases involving mortgage fraud, wire fraud, consumer-loan fraud, counterfeit check fraud, identity theft, embezzlement, bank robberies, and various financial institution fraud.

3.   As a Special Agent with DOL OIG, I have conducted numerous investigations into criminal violations of both Title 29 and Title 18 of the United States Code. During this time, I have been either the lead agent or supporting agent on several investigations involving criminal schemes targeting the unemployment insurance ("UI") program through the filing of false or fictitious UI claims. Based on my direct personal experience with these cases, I have become familiar with the methods that criminals use to attack and exploit the UI systems as well as the criminals' reliance on the use of email and other internet or online tools and systems to facilitate that fraud. More recently, this type of fraud has often involved Pandemic Unemployment Assistance claims.

4.   The facts of this affidavit come from my personal involvement in this criminal investigation, my training and experience, information obtained from my review of financial, employment, internet service provider, and utility records; law

1

enforcement surveillances and review of information stemming from search warrants obtained and executed during an investigation of a large-scale UI fraud scheme operating in Metropolitan Detroit and various parts of Michigan. I have also been provided with information from other law enforcement agents and officials, including agents and officials from the State of Michigan Fraud Investigation Unit (SOM FIU), Department of Homeland Security OIG (DHS OIG) and the FBI. This affidavit does not contain all the facts developed to date in the underlying investigation and is being submitted for the limited purpose of establishing probable cause to secure a criminal complaint and arrest warrant for RAY ANTHONY EDDINGTON.

5.   Based on my training and experience and the facts set forth in this affidavit, I submit that there is probable cause to believe that RAY ANTHONY EDDINGTON has committed federal crimes, including but not limited to, wire fraud (18 U.S.C. § 1343), conspiracy to commit wire fraud (18 U.S.C.§ 1349) and aggravated identity theft (18 U.S.C. § 1028A).

SUMMARY

6.   DOL OIG, DHS OIG and the FBI, are investigating a large-scale Pandemic Unemployment Assistance (PUA) fraud conspiracy, facilitated by multiple former State of Michigan (SOM) Unemployment Insurance Agency employees/contractors, (hereafter, Target Employees), and multiple other co-conspirators. The investigation has shown that the Target Employees accessed and/or altered over 400 PUA claims outside the scope of their duties, resulting in the outlay of over $5 million in UI benefits, including Pandemic Unemployment Assistance benefits. Those alterations included discarding various system generated fraud flags associated with those claims, to assure payments were issued. Without the Target Employees' alterations, many of those claims would not have been approved or paid. A review of internal SOM records also confirmed that some of claim accounts altered by the employees, contained fraudulent passports, driver's licenses, and social security cards, and that some of the employees themselves, uploaded those fraudulent documents to the claim accounts. This affidavit will detail information regarding one of the Target Employees, Target Employee 1, and her associate, RAY ANTHONY EDDINGTON (hereafter, EDDINGTON), and will not detail all information obtained regarding all identified targets at this stage of the investigation.

7.   The SOM FIU reviewed Target Employee 1's work activity and identified several anomalies in her activity, including that many of the claims she accessed and altered were not her assigned work items, and that she had accessed those claims outside the scope of her assigned duties. SOM FIU records indicated Target Employee 1 used her employee access to make changes to multiple claimant accounts, including uploading identification documents, with no evidence Target Employee 1 had spoken with the claimant to verify required information, nor that the claimant had contacted SOM.

8.   Financial records obtained during the investigation showed that during the time period the Target Employees are suspected of engaging in a fraudulent criminal conspiracy, the Target Employees were sending and receiving payments to one another, as well as receiving payments from some individuals associated with the altered PUA claim accounts. One of those individuals was identified as EDDINGTON. Agents obtained Cash App records documenting incoming and outgoing payments for Target Employee 1's Cash App account. Those records showed multiple payments from EDDINGTON to Target Employee 1's account.

9.   Agents obtained SOM UI/PUA claim records which confirmed EDDINGTON filed a PUA claim on April 21, 2021. Internal SOM records confirmed Target Employee 1 accessed and altered EDDINGTON's claim for payment, outside the scope of her assigned duties, resulting in EDDINGTON receiving $24,140 in PUA funds, to which he was not entitled.

10.   SOM FIU also reported Target Employee 1 uploaded suspected fraudulent identity documents for multiple PUA claims while logged into her SOM employee account, including but not limited to, claims filed under the names R.C. and J.F.

11.   I reviewed ATM surveillance images from Bank of America (hereinafter, BOA), of withdrawals made on various UI/PUA claim accounts associated with Target Employee 1's unauthorized alterations. At this stage of the investigation, I identified EDDINGTON withdrawing funds from multiple accounts. As noted below, EDDINGTON was positively identified in surveillance footage withdrawing funds from R.C.'s account, and an individual consistent with EDDINGTON's physical appearance and driving a vehicle associated with EDDINGTON is seen on surveillance footage withdrawing funds from J.F.'s account.

UNEMPLOYMENT INSURANCE BACKGROUND

12.   The Social Security Act of 1935 initiated the federal and state Unemployment Insurance system. The system provides benefits to individuals who are unemployed for reasons beyond their control. The purpose of the Unemployment Insurance system is to lessen the effects of unemployment through cash payments made directly to laid-off workers, and to ensure that life necessities are met on a weekly basis while the worker seeks employment. In the State of Michigan, the Unemployment Insurance system is administered by the Unemployment Insurance Agency, which is part of the State of Michigan's Department of Labor and Economic Opportunity.

13.   State unemployment systems and benefits are joint state and federal enterprises largely financed by taxes on private employers located in that state. As of the time of this application, the federal government has provided significant supplemental benefits to the states because of the COVID-19 pandemic. Beginning in, or about, March 2020, the Families First Coronavirus Response Act; Coronavirus Aid, Relief, and Economic Security Act; and the American Rescue Plan Act of 2021, have created federal programs that allowed for the significant outlay of federal funds to the states, to offset the historic need for unemployment benefits by the American workforce, including in the State of Michigan and in the Eastern District of Michigan. Collectively, these benefits are referred to as Pandemic Unemployment Assistance (PUA).

14.   Normally (in the absence of fraud), an unemployed worker initiates an Unemployment Insurance claim. This can be accomplished by submitting a claim in person, over the telephone, or via the Internet. Currently, most Unemployment Insurance claims are filed online via the Internet through the Unemployment Insurance Agency's website. To be eligible for Unemployment Insurance benefits, the worker must demonstrate a certain level of earnings in several quarters immediately preceding the application. The number of benefits that an Unemployment Insurance claimant might be eligible for depends on a variety of factors, including but not limited to, the length of his or her previous employment and the amount of wages he or she earned.

15.   The State of Michigan Unemployment Insurance Agency will either approve or reject an Unemployment Insurance claim based on the application made by the unemployed worker. If the State of Michigan Unemployment Insurance

Agency approves an Unemployment Insurance claim, the claimant is required to re-certify the claim via telephone or Internet at various times during the life of the claim. The worker must also certify that he or she is still unemployed and actively seeking work.

16.   Unemployment benefits are provided to a claimant through a debit card, issued by BOA, which maintains the claimants name, and is mailed to the claimant's provided address, through the U.S. Postal Service, or through Electronic Funds Transfers (EFTs) through his or her bank routing and account number. These EFTs originate from one or more accounts maintained by the Michigan Unemployment Insurance Agency at Bank of America, N.A., which is a subsidiary of Bank of America Corporation, a bank holding and financial holding company headquartered in Charlotte, North Carolina. All EFTs of Unemployment Insurance benefits to Michigan Unemployment Insurance claimants, whether via a BOA-provided debit card or via a claimant-provided bank account, involve the transmission of electronic signals through one of BOA's two data centers, which are located in Virginia and Texas, and from those data centers to banks located in Michigan. These are interstate wire communications.

Unemployment Insurance – Fraud Prevention

17.   In an effort to prevent and otherwise inhibit fraud, the State Workforce Agencies (SWA) capture certain data surrounding the interaction between an individual and the UI system. Each time a claim is accessed in the system, it creates a digital footprint. Although states utilize their own unique systems, many times the data that is collected includes the dates, times, IP address, and Media Access Control (MAC) address, associated with a device accessing a claim. The SWA systems tie this information to the user-entered information captured to facilitate the claim (i.e. name, address, social security number, BOA or other bank account numbers, bank routing numbers, etc.). It is through the analysis of this data that the SWAs and investigating agents can identify fraudulent trends and tendencies associated with certain claims.

18.   The SOM Fraud Manager system scores every UI claim once filed. Based on that system generated score, the system will flag a claim as potentially fraudulent, defined as a fraud stop, and will require additional information from the claimant and a review by an employee to verify that information, prior to approval and payment processing. There are various system generated fraud stop indicators, one of which includes an identification verification (IDV), which

requires the claimant to provide proof of identification and a review by an employee, prior to approval and payment issued on that claim.

19.   Additionally, the SOM UIA captures certain external data surrounding the interaction between an individual and the UIA system named the Michigan Integrated Data Automated System (MiDAS). Each time a claim is accessed in MiDAS, a digital footprint is created. Some of the data that the SOM collects includes the dates, times, Internet Protocol (IP) address, and Media Access Control (MAC) address associated with the device accessing the claim. SOM ties this information to the user-entered information captured to facilitate the claim (i.e. name, address, social security number, BOA or other bank account numbers, bank routing numbers, etc.). MiDAS also utilizes certain proprietary algorithms that automatically identify and stop possible fraud based on whether or not a claim exhibits fraud indicators that exceed a designated threshold. Agents also note that humans who review claims and conclude that the payments may be involved in fraud can also take action to stop payment of the claims. For the remainder of this affidavit, the investigating agent will refer to the process detailed above as a fraud-stop.

20.   In an effort to prevent and otherwise inhibit internal fraud or insider threats, SOM UIA captures certain internal data surrounding the interaction between SOM employees, contractors, consultants and MiDAS, which details any insider/employee who touches, alters, or otherwise modifies a claim. SOM can attribute an employee's actions to a particular individual, as those accessing the system are required to enter unique credentials. SOM also maintains workflow logs for its employees that detail which claims are assigned to a particular employee. Additionally, SOM maintains call logs to document telephonic contact between employees and claimants. The workflow logs and call logs detail whether an employee had a legitimate reason to access or modify a claim.

21.   Investigators from SOM FIU have the ability to access and review the data maintained for both external and internal actors in MiDAS. It is through the analysis of this data that investigating agents can identify fraudulent trends and tendencies associated with certain claims.

PROBABLE CAUSE

22.   The SOM FIU reviewed Target Employee 1's work activity in MiDAS through her unique SOM credentials and username. That activity

determined that between April of 2020 and November of 2021, Target Employee 1 electronically accessed, altered, and/or approved various UI and PUA claims, outside the scope of her assigned duties and responsibilities. Those alterations included removal of various fraud-stops, including identification verification (IDV) fraud-stops, in turn releasing payments on those claims that would not have been issued otherwise. Additionally, Target Employee 1 uploaded fraudulent identification documents, including driver's licenses, social security cards and U.S. passports, to multiple fraudulent PUA claims, including during the time she was logged into MiDAS.

23.   The SOM FIU confirmed that employees can upload identification documents on behalf of claimants on occasions, but that Target Employee 1 did not upload those documents through the normal process as an employee, but rather uploaded those documents specifically to the claim, circumventing the employee process. The following are examples of the fraudulent PUA claims altered by Target Employee 1 that contained fraud-stops, including EDDINGTON'S.

RAY EDDINGTON CLAIM

24.   I obtained and reviewed records from the SOM FIU documenting details of EDDINGTON's PUA claim. Those records confirmed that a PUA claim was filed on April 21, 2020 in EDDINGTON'S name. SOM internal access records showed Target Employee 1 accessed EDDINGTON'S claim approximately 494 times, between April 2020 and August 2021, outside the scope of her assigned duties, including 11 times through her identified IP address. SOM Records indicate that Target Employee 1 was never assigned to work on Eddington's claim. During that access, Target Employee 1 discarded Employment Verification and Fraud Investigation fraud-stops placed on EDDINGTON'S account, even though he had no proof of wages as required. Additionally, the SOM FIU confirmed that on July 13, 2020, documents were uploaded to EDDINGTON's account through Target Employee 1's identified IP address. The SOM FIU determined the documents were uploaded while Target Employee 1 was logged into her work computer, because they compared that IP address with Target Employee 1's VPN access that day, which showed at the same time the documents were uploaded, she was logged into the SOM system through that same IP address.

25.   Following Target Employee 1's unauthorized alterations, $24,140 in PUA benefits were issued to EDDINGTON to which he was not entitled. The SOM confirmed out of the $24,140, $2,991.60 was garnished to Friend of the

Court debts owed by EDDINGTON, and the remaining $21,148.40 was disbursed to EDDINGTON via a BOA debit card.

R.C. Claim

26.   On June 28, 2020, a PUA claim was filed under the name R.C. On that same day, a system generated IDV was placed on the account, indicating proof of identification and verification was needed prior to approval and payment processing.

27.   SOM FIU reported the following internal actions on R.C.'s account: Between July 5, 2020, and July 13, 2020, Target Employee 1 accessed R.C.'s claim nine times, outside the scope of her assigned duties, including through a search of his specific social security number. SOM Records indicate that Target Employee 1 was never assigned to work on R.C.'s claim. During this time, R.C.'s claim indicated an IDV stop was hindering approval and payment on his claim.

28.   On July 14, 2020, Target Employee 1 accessed R.C.'s claim through her internal access in MiDAS and directly uploaded a MI DL and social security (SS) card to his claim, outside the scope of her assigned duties. Target Employee 1 then assigned the IDV to her name and adjudicated/closed the IDV flag on the account. Target Employee 1 then reviewed the payment section of the claim, which confirmed the payment had been changed to pending. An hour later, Target Employee 1 re-entered the claim and discarded a failed to accept issue. SOM FIU confirmed that if this issue is placed on the account, it means the claimant refused a job offer and would be deemed ineligible to receive funding.

29.   On July 15, 2020, a system-generated Benefit Payment Review fraud stop was placed on R.C.'s account, because the claim payment anticipated was an anomaly, due to the high financial amount. On August 10, 2020, Target Employee 1 went into R.C.'s claim and rejected the Benefit Payment Review fraud stop, which authorized and released payment on that claim that following day.
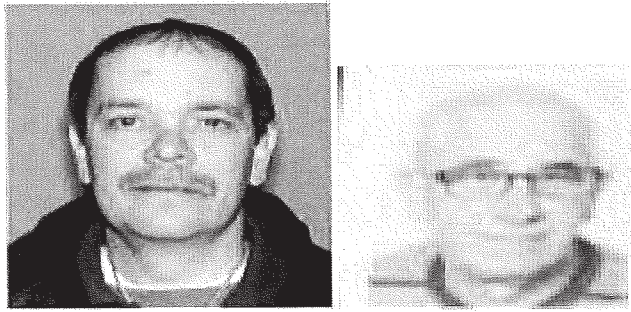
30.   On November 20, 2020, another IDV stop was generated on R.C.'s account after his claim was reopened, meaning that it was reactivated for potential claim payment after a stagnant period of inactivity. Records obtained throughout this investigation confirmed the IP address used to access R.C.'s account this day was registered to Target Employee 1's residence.

31.   On December 3, 2020, Target Employee 1 went into R.C.'s claim and discarded the IDV flag. That same day, a system generated fraud investigation fraud stop was placed on R.C.'s account. On January 25, 2021, Target Employee 1 discarded the fraud investigation.

32.   On February 11, 2021, a PUA Employment Verification Issue listed as "Ineligible" was placed on R.C.'s claim, due to lack of documentation submitted by the claimant. On March 5, 2021, Target Employee 1 closed the PUA Employment Verification Issue, outside the scope of her assigned duties, even though no documentation was sent in.

33.   Overall, SOM FIU confirmed that Target Employee 1 accessed R.C.'s claim approximately 284 times, during which she discarded numerous fraud-stops placed on the account, which were all outside the scope of her assigned duties. Target Employee 1's actions allowed a total of $33,420 in PUA funds to be paid on R.C.'s claim between August 7, 2020, and August 25, 2021.

34.   On February 2, 2022, Agents conducted various law enforcement database searches of R.C. with the name, DOB, and SSN provided on his PUA claim. Those records showed that R.C. maintained an expired MI DL and he had no ties to the residential address provided on his claim, 27*** Aberdeen, Southfield, MI. Agents obtained a copy of R.C.'s most recent expired MI DL and compared the photograph to the DL uploaded by Target Employee 1. That review showed that the photographs did not match, as shown below, indicating the documents Target Employee 1 uploaded to R.C.'s claim were likely fraudulent. See below comparison between expired Michigan DL photo for the true R.C. (left) and DL uploaded as part of claim made in his name (right):

J.F. Claim

35.   On June 24, 2020, a PUA claim was filed under the name J.F., at which time a system generated IDV was placed on the account, indicating proof of identification and verification was needed prior to approval and payment processing.

36.   On July 14, 2020, Target Employee 1 accessed J.F.'s claim through her internal access in MiDAS, and uploaded a DL and SS card, outside the scope of her assigned duties directly after Target Employee 1 closed the IDV, changing the status to eligible, again outside the scope of her assigned duties. Target Employee 1 proceeded to alter the claim multiple times to remove various other fraud stops that were stopping payment on the claim, all outside the scope of her assigned duties. Target Employee 1's actions generated another IDV, which Target Employee 1 immediately discarded again.

37.   SOM Records indicate that Target Employee 1 was never assigned to work on J.F.'s claim.

38.   SOM FIU reported that J.F.'s claim had another IDV fraud stop placed on his claim account on November 20, 2020, due to J.F. reopening the claim on IP address 24.127.17.126 (Target Employee 1's residential address's IP address.) On December 3, 2020, Target Employee 1 entered J.F.'s claim, and discarded the IDV fraud stop, outside the scope of her assigned duties, issuing payment again.

39.   Overall, SOM FIU reported that Target Employee 1 accessed J.F.'s claim approximately 297 times between June 24, 2020, and April 22, 2021, and that Target Employee 1's access and alterations to that claim, were outside the scope of her assigned duties. Target Employee 1's alterations allowed a total of

$23,300.00 in PUA funds to be paid on J.F.'s claim between July 23, 2020, and March 29, 2021.

40.   On February 2, 2022, Agents conducted various law enforcement database searches of J.F. with the name, DOB, and SSN provided for the PUA claim. Records showed that J.F.'s MI DL was expired, and he had no ties to the residential address provided on his claim, 27*** Aberdeen, Southfield, MI. Agents obtained a copy of J.F.'s most recent expired MI DL and compared the photograph to the DL uploaded by Target Employee 1. See below comparison between expired Michigan DL photo for the true J.F. (left) and DL uploaded as part of claim made in his name (right):

IDENTIFICATION OF RAY EDDINGTON

41.   SOM FIU obtained records from BOA for the debit cards issued in response to the PUA claims accessed and/or altered by Target Employee 1. During that review, it was identified that various cash withdrawals were made from the BOA accounts. SOM FIU requested surveillance footage and images from BOA, of those cash withdrawals from those accounts. To date I have reviewed surveillance footage and images from cash withdrawals on numerous BOA PUA claim accounts associated with Target Employee 1's alterations. At this stage of my review, I identified EDDINGTON making cash withdrawals from multiple different claimant BOA accounts associated with Target Employee 1. EDDINGTON was positively identified in surveillance footage withdrawing funds from R.C.'s account, and an individual consistent with EDDINGTON's physical appearance is seen on surveillance footage withdrawing funds from J.F.'s account.

42.   The following is a summary of withdrawals pertaining to R.C. and J.F.'s accounts.

43.   BOA provided surveillance footage of the financial withdrawals associated with R.C.'s BOA debit card, between April 28, 2021, and June 8, 2021, which that took place within the EDMI. I reviewed all surveillance footage and identified EDDINGTON making numerous cash withdrawals from R.C.'s debit card. I identified EDDINGTON by comparing EDDINGTON's SOM DL with the BOA surveillance footage, as well as the identification of the vehicle captured. The vehicle license plate in certain surveillance photos was identified as EGG **71. Agents previously identified EGG **71 as a vehicle associated with EDDINGTON at his residential address listed on his DL and used on his PUA claim, 22*** S. Bellwood Dr. Southfield, MI, 48034. Specifically, I conducted law enforcement database queries, which confirmed EGG **71 is registered to a black 2020 Ford Explorer with a VIN ending in 9210 and is registered to a business named "Cab West LLC" at EDDINGTON'S same address. Records show that EDDINGTON has previously been the registered owner of this vehicle. I also identified record of a local police traffic stop with EDDINGTON driving this vehicle in April 2021. Records show that another vehicle currently registered to EDDINGTON has a secondary owner listed as "Cab West LLC."

44.   Below is a copy of EDDINGTON's State of Michigan Driver's license photo retrieved from the State of Michigan Secretary of State System (Figure 1), as well as images captured from the BOA surveillance footage, showing the person who conducted various cash withdrawals on R.C.'s account (Figure 2).

Figure 1. Ray Anthony Eddington DL photo.

Figure 2- BOA ATM Surveillance

45.   BOA provided surveillance footage of the financial withdrawals associated with J.F.'s BOA debit card, between April 09, 2021, and April 12, 2021, which took place in the ED-MI. I reviewed the surveillance footage and identified an individual consistent with the physical appearance of EDDINGTON as the individual that made numerous cash withdrawals from J.F.'s account. Certain surveillance photos of withdrawals from J.F.'s account also show the individual whose physical appearance is consistent with that of EDDINGTON driving the same black Ford Explorer with license plate EGG **71 that is associated with EDDINGTON and discussed above.

46.   Below is a copy of EDDINGTON's State of Michigan Driver's license photo retrieved from the State of Michigan Secretary of State System (Figure 3), as well as images captured from the BOA surveillance footage, showing the person who conducted cash withdrawals on R.C.'s account (Figure 4).

Figure 3- Ray Anthony Eddington DL photo.

Figure 4- BOA ATM Surveillance

CONFIRMED ASSOCIATION BETWEEN TARGET EMPLOYEE 1 AND EDDINGTON

47.   On February 16, 2022, Agents executed a search warrant at Target Employee 1's residence. During the execution of the search warrant, Target Employee 1 was interviewed and provided a voluntary statement. Target Employee 1 identified EDDINGTON as her daughter's father. Target Employee 1 admitted she accessed and altered EDDINGTON'S PUA claim and acknowledged she knew it was wrong. Target Employee 1 acknowledged she received payments from EDDINGTON through Cash App, but claimed the payments were for their daughter, not for altering his claim account. During the interview, Agents described records that showed she uploaded fraudulent driver's licenses and social security cards to some of the accounts she altered for payment, including claims filed under the names of R.C. and J.F. Target Employee 1 stated she did not know who R.C. nor J.F. were, denied creating the fake identification cards, but claimed

19

that she received the cards from someone else. Target Employee 1 would not disclose who.

CONCLUSION

48.   Based on the forgoing, there is probable cause to believe that RAY ANTHONY EDDINGTON has committed federal crimes, including but not limited to, wire fraud (18 U.S.C. § 1343), conspiracy to commit wire fraud (18 U.S.C. § 1349); aggravated identity theft (18 U.S.C. § 1028A), in connection with a scheme to defraud the federal/state unemployment insurance programs, resulting in his receipt of unemployment benefits by means of false and fraudulent pretenses and representations.

REQUEST FOR SEALING

49.   If further request the Court order that all papers in support of this application, including the affidavit and arrest warrant, be sealed until further order of the court. These documents discuss an ongoing criminal investigation is neither public nor known to all potential targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets opportunity to destroy or tamper with evidence, change patterns of behavior, notify co-conspirators, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Elizabeth Weitzel
Special Agent
U.S. Department of Labor –
Office of Inspector General

Sworn to before me and signed in my
presence and/or by reliable electronic means.

Honorable Anthony P. Patti
United States Magistrate Judge
Date: January 25, 2023